STUDENT ID NO

MULTIMEDIA UNIVERSITY □□□□□□□□□□

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2019/2020

TMI 3231 – MALWARE AND INTRUSION DETECTION

(All sections / Groups)

29 FEBRUARY 2020
2.30 – 4.30 PM
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 8 pages with 5 Questions including the cover page.

2. Attempt **ALL FIVE** questions. All questions carry equal marks and the distribution of the marks for each question is given.

3. Please print all your answers in the Answer Booklet provided.

QUESTION 1

Please attempt **ALL** multiple choice questions. (12 marks)

1. The quality/state of being genuine or original rather than a reproduction/copy and is considered such when it is in the same state as when it was created, placed, stored or transferred. Which critical characteristics of information does this statement refer to?
   a. Authenticity
   b. Accuracy
   c. Confidentiality
   d. Availability

2. Which of the below is NOT a category of attack?
   a. Malware
   b. Keyloggers
   c. Intrusion
   d. Blocking

3. "A common virus infection technique uses the principle of inserting virus code at the front of host programs". Such viruses are called _____.
   a. Cavity virus
   b. Overwriting virus
   c. Prepending virus
   d. Appending virus

4. Which of the followings is NOT a security tasks done by the Firewall?
   a. Protecting against hacking
   b. Restricting employee access to external hosts
   c. Providing centralization
   d. Enabling access from outside the network

5. The first four bits in the header of an IP packet denotes __________.
   a. Version
   b. Internet Header Length
   c. Type of Service
   d. Fragment Offset

Continued...

6. Scalability is important in configuring a firewall. Which of the statements below is NOT correct to describe scalability?
   a. Adapt to the changing needs of the organization.
   b. Faster data transmission.
   c. Upgrade software and hardware as needed.
   d. Increase the need for firewall resources.

7. The statements below describe how proxy servers are different from packet filters EXCEPT:
   a. Create much more detailed log file listings than packet filters.
   b. Rebuild the packet with new source IP information.
   c. Less critical to network communications than packet filters.
   d. Attacks that can start with invalid packet data never reach the internal host.

8. Memory considerations is essential in selecting the host machine. Which of the followings is FALSE regarding memory considerations?
   a. Create a page file on hard disk.
   b. Hard disk storage space should be multiterabyte.
   c. RAM is always important when operating server.
   d. Need multiterabytes worth of RAM.

9. "It is part of a wireless audit. It finds Rogue access points. It finds Evil Twins". This statement is referred to ____________.
   a. Wardriving
   b. Bluesnarfing
   c. Reverse Proxies
   d. Tailgating

10. ______________ cipher rearranges the values within a block to create the ciphertext during the encryption process.
   a. Transposition
   b. Substitution
   c. XOR
   d. Vernam

Continued...

11. Which VPN Topology is displayed in Figure 1?

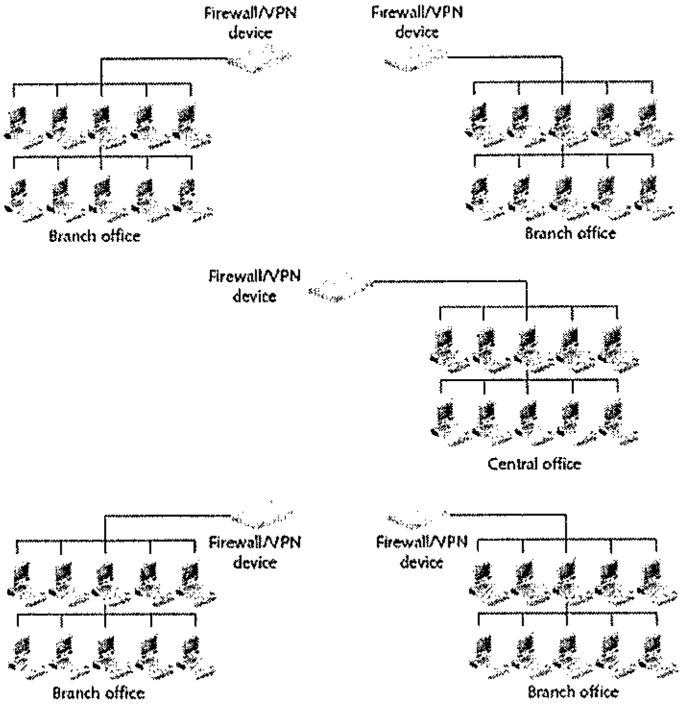


Figure 1.

a. Mesh Configuration
b. Hybrid Setup
c. Hub-and-Spoke Configuration
d. Point-to-Point Setup

12. ____________ infect both executable files and boot sectors.

a. Binary file viruses
b. Script file viruses
c. Multipartite viruses
d. Macro viruses

Continued...

QUESTION 2

a) There are a few unified processes of information security. Refer to the Table 1, what are the **TWO (2)** missing processes?

Table 1

1	
2	
3	Personal security
4	Operational security
5	Communication security

(2 marks)

b) What is operational security (OPSEC)? Give any example of scenario to illustrate the risk of operational security.

(4 marks)

c) Crimeware can be distributed in many ways. It is important to know the ways of distribution before taking any preventive actions. List **THREE (3)** ways that the Crimeware is being distributed.

(3 marks)

d) What is the shoulder surfing? Name **TWO (2)** countermeasures of shoulder surfing.

(3 marks)

Continued...

QUESTION 3

a) A packet filter has a set of rules with accept or deny actions. When the packet filter receives a packet of information, the filter compares the packet to your preconfigured rule set. Identify **FOUR (4)** common rules for Packet-filtering.

(4 marks)

b) Application proxies provide one of the most secure types of access you can have in a security gateway. Describe how an application proxy works.

(4 marks)

c) Refer to Figure 2 below, discuss the advantages when you place the Intrusion Detection and Prevention Systems in the Location 3 and Location 4.

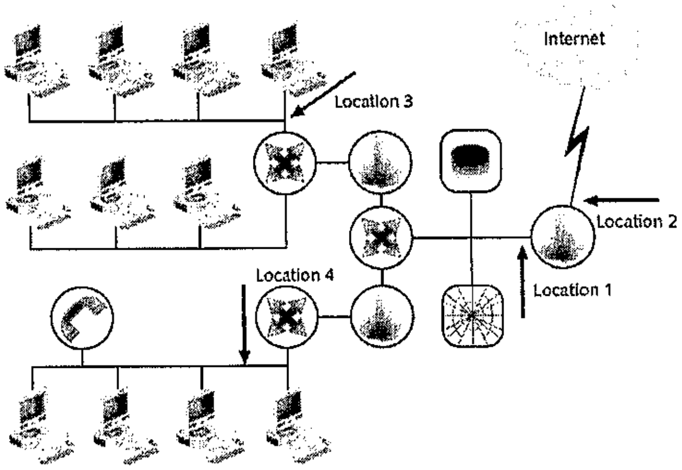


Figure 2

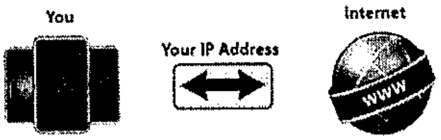
(4 marks)

Continued...

QUESTION 4

a) The diagram below shows a network without using proxy server.

WITHOUT PROXY SERVER:



i. If you are going to implement the proxy server into the network, how will you place the proxy server? Illustrate your answer by modifying the diagram.

(1 mark)

ii. Explain how the proxy server works in a network.

(2 marks)

iii. What are the advantages of applying the proxy server in a network? Suggest **THREE (3)** advantages.

(3 marks)

b) JX Corporation would like to install a Bastion Host in its network. What are the main considerations when selecting a Bastion Host's processor speed and operating system? Justify your answer.

(4 marks)

c) Remote access is the ability to access a computer or a network remotely through a network connection. Users access systems remotely through dial-up or Virtual Private Network. Differentiate these two remote access methods.

(2 marks)

Continued...

QUESTION 5

a) Modern networked business environments require a high level of security to ensure safe and trusted communication of information between various organizations. An Intrusion Detection System (IDS) acts as an adaptable safeguard technology for system security after traditional technologies fail. There is a wide array of IDS and always we can see the terms HIDS, NIDS, Signature-based and Anomaly-based. Describe the differences of these terms and how can you relate each of these terms to IDS?

(6 marks)

b) "*Significant rise in the number of cyber-attacks and surge in demand for cloud-based security solutions is expected to boost the Virtual Private Network (VPN) market over the forecast period.*" Based on the statement, we understand the importance of VPN in network configuration. Why is VPN market having significant rise comparing to the leased line market?

(2 marks)

c) Alice and Bob use asymmetric key cryptography to securely communicate with each other. The file that contains the Alice's private key is corrupted. Therefore, Alice does not have access to her private key anymore. Can Alice still encrypt messages to Bob? Justify your answer.

(2 marks)

d) A company manager has requested his staff to use Kerberos protocol in order to strengthen the security of the company's network. In your opinion, how can Kerberos contribute to a stronger security?

(2 marks)

End of Paper